SIEMENS

Security information 1

Introduction 2

Installation 3

SIMATIC

Industrial Software
SIMATIC S7 F Systems Library V1.3 SP4

Readme

V6.4
A5E50890130-AA

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E50890130-AA
Ⓟ 04/2021 Subject to change

Copyright © Siemens AG 2021.
All rights reserved

Table of contents

1 Security information 5
2 Introduction 7
3 Installation 9

Security information

1

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit
https://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under
https://www.siemens.com/industrialsecurity.

Introduction

2

Read the following instructions carefully because they contain important information for the installation and operation of the SIMATIC S7 F Systems Library that you must observe.

Installation 3

Software requirements

The same software requirements as for SIMATIC S7 F Systems V6.4 apply. Please also observe the SIMATIC S7 F Systems V6.4 readme file.

Installation

The setup program will guide you through the installation process step-by-step. You can always move to the next window or return to the previous one from each position. To install the optional package, proceed as follows:

1. Ensure that the software requirements are fulfilled.
2. Close all applications in STEP 7 before you start the setup program.
3. Start the SETUP.EXE program on the installation storage medium.
4. Follow the instructions of the setup program.

Password of the S7 F Systems Library

The password for the included S7 F Systems Library is:

- Fsys_v63

Uninstalling

It is recommended not to uninstall the SIMATIC S7 F Systems components as this can lead to problems with your configuration.

If you want to remove SIMATIC S7 F Systems or one of the components, place it on a basic image of your system and reinstall the required components.